La protecció de dades personals a la nostra entitat.

Formació teòrica i pràctica per conèixer els requisits per complir la LOPD a la nostra entitat

Dijous 17 de novembre, de 18 a 20:30 h a la Sala Noble de la Casa Olivella (Plaça de la Vila 12)

Ramon Arnó, advocat de la Consultoria Sagaris

ramon@sagaris.cat

INDEX

1.- EL MATERIAL FORMATIU 3
2.- LES NOTICIES DELS MITJANS DE COMUNICACIÓ 4
3.- EXEMPLES D'INFRACCIONS D'EMPRESES 5
4.- LA PROTECCIÓ DE DADES PERSONALS 6
5.- LES OBLIGACIONS DEL RESPONSABLE PRÈVIES AL TRACTAMENT 9
5.1.- CREAR, MODIFICAR I SUPRIMIR ELS FITXERS 9
5.2.- ADOPTAR MESURES DE SEGURETAT 10
6.- LES OBLIGACIONS DEL RESPONSABLE DURANT EL TRACTAMENT 15
6.1.- QUALITAT DE LES DADES 15
6.2.- INFORMAR LES PERSONES TITULARS DE LES DADES. .. 15
6.3.- OBTENIR EL CONSENTIMENT 16
6.4.- ACOMPLIR AMB EL DEURE DE SECRET 17
5.5.- CONTROLAR LES CESSIONS DE DADES 21
5.6.- TRANSFERÈNCIES INTERNACIONALS DE DADES 22
5.7.- ENCARREGAT DEL TRACTAMENT 24
6.- LES OBLIGACIONS DEL RESPONSABLE DESPRÉS DEL TRACTAMENT 26
6.1.- CANCEL·LACIÓ 26
7.- ELS DRETS DE L'AFECTAT: A.R.C.O 26
8.- LES OBLIGACIONS DEL PERSONAL (document de seguretat) 28
9.- LA RESPONSABILITAT 34
9.1.- ASPECTES CIVILS 34
9.2.- ASPECTES PENALS 34
9.3.- ASPECTES ADMINISTRATIUS 35
9.4.- ASPECTES LABORALS 35
10.- EL PROTOCOL D'ÚS DE LES TECNOLOGIES DE LA INFORMACIÓ 36
11.- DECÀLEG PER LA PROTECCIÓ DE DADES PERSONALS 37

1.- EL MATERIAL FORMATIU

- **Vídeo "els llums funcionen":**
  - **http://www.avpd.euskadi.eus/s04-5249/es/contenidos/informacion/documentos_difusion/es_difusion/r01hRedirectCont/contenidos/informacion/documentos_difusion/es_difusion/luces.html**

2.- LES NOTICIES DELS MITJANS DE COMUNICACIÓ

- **Robat d'un ambulatori un ordinador amb dades confidencials de 15.000 malalts.**
  - **http://elpais.com/diario/2007/03/29/madrid/1175167455_850215.html**
- **Protecció de dades inicia l´investigació de Sánchez Romero per l'escàndol dels currículums.**
  - **http://www.belt.es/noticias/2002/02_julio/08_12/10_sanchezromero.htm**
- **Subhasten a ebay un ordinador amb milions de dades bancàries.**
  - **http://www.elmundo.es/navegante/2008/08/26/tecnologia/1219744249.html**
- **Multa de protecció de dades per un 'e-mail' no desitjat.**
  - **http://elpais.com/diario/2000/02/11/sociedad/950223616_850215.html**
- **500 analítiques localitzades en la brossa.**
  - **http://www.madridiario.es/2008/Septiembre/madrid/madrid/98600/puerta-de-hierro-500-analiticas-basura.html**
- **Google haurà d'oblidar el teu passat.**
  - **http://elpais.com/diario/2008/01/22/sociedad/1200956401_850215.html**
- **Condemnat un metge a 3 anys de presó per accedir a l'historial d'un company.**
  - **http://www.diariodemallorca.es/secciones/noticia.jsp?pRef=2009021400_10_436037__Sucesos-Condenado-medico-carcel-acceder-historial**

3.- EXEMPLES D'INFRACCIONS D'EMPRESES

- **Vulneració del deure de secret mitjançant trucades a familiars per el recobrament de deutes.**
- **Difusió per un gimnàs d'un fitxer amb dades de 9.293 persones adjunt a un correu electrònic. Vulneració del deure de secret.**
- **Publicació de comunicat mèdic d'incapacitat d'una treballadora al perfil de Facebook de la seva empresa.**
- **Concurs de TV remet de forma massiva SMS no sol·licitats i sense mitjà d'oposició**
- **Recollida de dades de menors sense consentiment patern a lloc web.**
- **Correu electrònic amb adreça en obert de múltiples destinataris.**
- **Tractament a Facebook d'imatge de tercers.**
- **Sanció per crear un perfil fals de tercer en xarxa social.**
- **Codi d'usuari i contrasenya genèrica que permeten accés indiscriminat.**
- **Enviament sense còpia oculta de dades de deute a 129 afectats.**
- **Ús d'imatge de menor en cartell publicitari.**
- **Comunitat de propietaris difon imatges per Internet.**
- **Dades clínica dentista a EMULE.**
- **Transmissió dades de salut por fax.**
- **Falta mesures de seguretat a impressió de nòmines.**

4.- LA PROTECCIÓ DE DADES PERSONALS

- **Les dades personals són dels afectats, no de les empreses ni de les Administracions Públiques.**

- **Les dades personals valen molts diners.**

- **El dret a la protecció de dades es un dret fonamental (STC 292/2000)**

- **Hi ha dos figures importants:**
  - **el responsable del fitxer o tractament:**
    - **Ajuntament,**
    - **Supermercat,**
    - **Dentista,**
    - **Advocat**
  - **l'afectat: és la persona física titular de les dades.**

- **Hi ha moltes normes aplicables:**
  - **la LOPD -15/1999-,**
  - **el RLOPD –RD 1720/2007-,**
  - **la LSSICE –34/2002 els correus electrònics-**

- **Enllaç a tota la normativa (APDCAT)**
  - **http://www.apd.cat/es/contingut.php?cont_id=427&cat_id=122**
  -

- **Novetats a nivell europeu: el reglament 679/2016**

- **Un resum**
- **http://www.apd.cat/ca/contingut.php?cat_id=751&cont_id=704**
- **adaptació al mon digital**
- **no caldrà notificar els fitxers**
- **el dret a l´oblit**
- **el DPO**
- **notificar els escletxes de seguretat**
- **informe d´impacte sobre la privacitat**

- **Hi ha unes agències o autoritats encarregades de tutelar el dret a la protecció de dades de caràcter personal:**
  - **www.apd.cat**
  - **www.agpd.es**

- **La legislació s'aplica a:**
  - **el tractament de dades**
    - **demanar dades,**
    - **recollir-les en un paper,**
    - **cedir-les,**
    - **destruir-les.**
  - **personals, referides a persones físiques identificables**
    - **noms,**
    - **cognoms,**

        - **dni,**
        - **correu electrònic,**
        - **videovigilància,**
        - **fotografies,**
        - **número historia clínica,**
        - **adreça IP.**
    - **tant als fitxers manuals com als automatitzats.**

- **Hi ha dades molt protegides (també conegudes com sensibles):**
    - **ideologia,**
    - **religió,**
    - **creences,**
    - **afiliació sindical,**
    - **origen racial,**
    - **salut,**
    - **vida sexual,**
    - **infraccions penals i administratives,**
    - **violència de gènere.**

- **Compte amb el tractament de dades de menors de 14 anys (té una regulació específica).**

5.- LES OBLIGACIONS DEL RESPONSABLE PRÈVIES AL TRACTAMENT

5.1.- CREAR, MODIFICAR I SUPRIMIR ELS FITXERS

- **Quins són els fitxers habituals en una empresa?**
  - **Personal / recursos humans**
  - **Currículums**
  - **Clients / Facturació**
  - **Proveïdors**
  - **Comptabilitat**
  - **Contactes**
  - **Newsletter**
  - **Internet**
  - **videovigilància**

- **on?**
  - **Ampa: apdcat**
    - **Fitxers de titularitat privada**
      - **http://www.apd.cat/media/resolucio/ca_res_pdfresolucio442.pdf#search=ampa**
      - **http://www.apd.cat/media/resolucio/ca_res_pdfresolucio214.pdf#search=ampa**
  - **La resta: agpd**
    - **asociacion xxxx mulleres luguesas contra a violencia de xenero**
      - **http://www.agpd.es/portalwebAGPD/resoluciones/procedimiento_apercibimiento/procedimiento_apercibimiento_2016/common/pdfs/A-00146-2016_Resolucion-de-fecha-06-10-2016_Art-ii-culo-5.1-LOPD.pdf**

- Asociación de Empresarios de Tecnologías de l Información y Comunicaciones de Andalucía (ETICOM)
    - http://www.agpd.es/portalwebAGPD/resoluciones/procedimientos_sancionadores/ps_2016/common/pdfs/PS-00565-2015_Resolucion-de-fecha-01-04-2016_Art-ii-culo-21-LSSI_Recurrida.pdf

- Respecte dels fitxers nous:
    - Abans d'iniciar qualsevol tractament de dades personals, el responsable del fitxer ha de notificar el fitxer, i sol·licitar-ne la inscripció al registre de protecció de dades corresponent i obtenir-ne la inscripció.

- Respecte dels fitxers ja existents
    - Quan hi hagi canvis en el fitxer respecte de la inscripció inicial, s'ha de fer la modificació al registre de protecció de dades corresponent.
    - Si se cessa en l'ús del fitxer, s'ha de suprimir.
    - Per tant, la modificació o la supressió del fitxer comporta fer-ne la notificació i la sol•licitud d'inscripció al registre de protecció de dades corresponent.

5.2.- ADOPTAR MESURES DE SEGURETAT

- Guia i model de document de seguretat
    - https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_SEGURIDAD_2010.pdf

- Quin és l'objectiu bàsic de les mesures de seguretat?

- **Garantir la seguretat de les dades personals i evitar l'alteració, la pèrdua, el tractament no autoritzat i l'accés no autoritzat a les dades personals.**

- **<u>Qui té el deure d'implantar les mesures de seguretat</u>?**
  - **El responsable del tractament és qui té el deure d'adoptar les mesures de seguretat i preveure tot allò que sigui necessari per garantir que les dades personals estan efectivament protegides**
  - **En determinades circumstàncies, aquest deure també afecta els anomenats encarregats del tractament.**

- **<u>On s'han d'aplicar les mesures de seguretat</u>?**
  - **als centres de tractament,**
  - **als locals,**
  - **als equips,**
  - **als sistemes,**
  - **als programes.**

- **<u>Quins tipus de fitxers o tractaments afecta</u>?**
  - **Amb caràcter general, les mesures de seguretat han de protegir les dades de caràcter personal, independentment de la seva ubicació o sistema de tractament.**
  - **Per tant, les mesures s'apliquen a tots els fitxers que continguin dades personals, tant si són automatitzats com si són en suport paper (no automatitzats).**

- **<u>Com s'estructuren les mesures de seguretat</u>?**
  - **El Reial decret 1720/2007, que aprova el Reglament de desenvolupament de la LOPD (RLOPD),**

dedica el títol VIII a les mesures de seguretat en el tractament de dades de caràcter personal.

- **En primer lloc, es regula una part general, que afecta tot tipus de tractaments i tots els nivells de seguretat (capítols I i II, articles 79 a 88).**
- **Després es tracta la regulació de les mesures de seguretat per als tractaments automatitzats, en què s'utilitza l'assignació de nivell de seguretat bàsic, mitjà o alt (capítol III, articles 89 a 104).**
- **Finalment, es regulen les mesures de seguretat per als tractaments no automatitzats, seguint el mateix esquema de nivells de seguretat (capítol IV, articles 105 a 114).**

- **<u>Tots els fitxers i tractaments necessiten les mateixes mesures de seguretat</u>?**
  - **No.**
  - **Hi ha tres nivells de seguretat, segons la naturalesa de la informació**
    - **nivell bàsic,**
    - **nivell mitjà,**
    - **nivell alt.**
  - **Però cal tenir en compte que els nivells de seguretat són acumulatius, de manera que en un fitxer de nivell alt s'han d'aplicar també les mesures previstes en els nivells bàsic i mitjà.**

- **<u>Com sabem les mesures de seguretat que cal aplicar en cada cas</u>?**
  - **Els tres nivells en què s'organitzen les mesures de seguretat, bàsic, mitjà i alt, s'apliquen en funció del tipus de dades objecte del tractament**
  - **Per a cada nivell es descriuen una sèrie de requeriments de protecció de les dades adreçats a**

determinar què és el que ha de procurar la mesura de seguretat.

- **<u>A quins fitxers i tractaments s'apliquen les mesures de nivell bàsic</u>?**
  - **A tots els que continguin dades personals.**
  - **També, en casos particulars:**
    - **a. Fitxers o tractaments de dades d'ideologia, afiliació sindical, religió, creences, origen racial, salut o vida sexual quan:**
      - **i. Les dades s'utilitzin amb l'única finalitat de fer una transferència de diners a les entitats de què els afectats siguin associats o membres.**
      - **ii. Es tracti de fitxers o tractaments no automatitzats en què, de forma incidental o accessòria, s'inclouen les dades sense tenir relació amb la seva finalitat.**
      - **iii. Fitxers o tractaments que continguin dades relatives a la salut quan es refereixin exclusivament al grau de discapacitat o a la simple declaració de la condició de discapacitat o invalidesa de la persona afectada, amb motiu del compliment dels deures públics.**

- **<u>A quins fitxers i tractaments s'apliquen les mesures de nivell mitjà</u>?**
  - **Als relatius a la comissió d'infraccions administratives o penals.**
  - **Als relatius a solvència patrimonial i crèdit.**
  - **A aquells els responsables dels quals siguin les administracions tributàries i es relacionin amb l'exercici de les seves potestats tributàries**
  - **A aquells els responsables dels quals siguin les entitats financeres amb finalitats relacionades amb la prestació de serveis financers.**

- **A aquells els responsables dels quals siguin les entitats gestores i serveis comuns de la seguretat social i es relacionin amb l'exercici de les seves competències.**

- **A aquells els responsables dels quals siguin les mútues d'accidents de treball i malalties professionals de la Seguretat Social.**

- **A aquells que continguin un conjunt de dades personals que ofereixin una definició de les característiques o de la personalitat dels ciutadans i que permetin avaluar determinats aspectes de la personalitat o del comportament d'aquests.**

- **Amb particularitats:**

  - **1. A aquells els responsables dels quals siguin els operadors que prestin serveis de comunicacions electròniques disponibles al públic o explotin xarxes públiques de comunicacions electròniques respecte de les dades de tràfic i les dades de localització. A aquests fitxers se'ls ha d'aplicar, a més, una mesura de nivell alt, la relativa al registre dels accessos a la informació que contenen.**

- **<u>A quins fitxers s'apliquen les mesures de seguretat de nivell alt</u>?**

  - **Als que es refereixen a dades d'ideologia, afiliació sindical, religió, creences, origen racial, salut o vida sexual**

  - **Als que continguin o es refereixin a dades recollides amb finalitats policials sense el consentiment de les persones afectades.**

  - **Als que continguin dades derivades d'actes de violència de gènere.**

6.- LES OBLIGACIONS DEL RESPONSABLE DURANT EL TRACTAMENT

6.1.- QUALITAT DE LES DADES

- Suposa complir amb un conjunt de principis durant el tractament de les dades:
  - Recollir només les dades necessàries per a la finalitat que es pretén.
  - No utilitzar les dades per a finalitats diferents de la que va generar la recollida.
  - Assegurar-se que les dades són exactes i actuals.
  - Cancel·lar les dades que siguin inexactes o incompletes i substituir-les d'ofici per les dades rectificades o completades.
  - Cancel·lar les dades quan hagin deixat de ser necessàries per a la finalitat per a la qual es van recollir. Això vol dir bloquejar les dades i després destruir o conservar.
  - Emmagatzemar les dades de manera que permetin l'exercici del dret d'accés.
  - No recollir dades per mitjans fraudulents, deslleials o il·lícits.

6.2.- INFORMAR LES PERSONES TITULARS DE LES DADES.

- És el dret que tot afectat té a conèixer, en qualsevol moment, què es fa amb les seves dades personals
- En concret, en el moment de la recollida de les dades s'ha d'informar la persona, d'una manera clara, sobre un conjunt d´aspectes següents:
  - L'existència d'un fitxer o tractament de dades de caràcter personal.

- La finalitat de la recollida.
- Els destinataris de la informació.
- La identitat i la direcció de la persona responsable del tractament.
- La possibilitat d'exercir els drets d'accés, rectificació, cancel·lació i oposició (coneguts per l'abreviatura ARCO).
- Si és obligatori o no respondre a les preguntes que es demanen
- Les conseqüències de proporcionar aquestes dades i les conseqüències de no proporcionar-les.

- Quan les dades es recullen en formularis, aquesta informació s'ha de fer constar
  - Aquí teniu alguns exemples:
    - Paper.
    - Tractament informàtic (web, correu electrònic, fax).
    - Telèfon (missatge gravat).
    - Càmeres de seguretat (cartells i clàusula d'informació).

6.3.- OBTENIR EL CONSENTIMENT

- El responsable del tractament ha d'obtenir el consentiment de la persona interessada per tractar les seves dades personals, tret d'aquells casos en què no calgui (hi ha excepcions com per exemple l'existència d'un contracte).
- El consentiment ha de ser lliure, informat, específic i revocable.
- Al responsable li correspon provar que disposa d'aquest consentiment.

6.4.- ACOMPLIR AMB EL DEURE DE SECRET

- El responsable del fitxer i els qui intervinguin en qualsevol fase del tractament de les dades de caràcter personal estan obligats al secret professional pel que fa a les dades i al deure de guardar-les.
- Aquestes obligacions subsisteixen fins i tot després d'haver acabat la relació amb el titular del fitxer o, si s'escau, amb el seu responsable.
- L'incompliment té conseqüències administratives, laborals i penals.
- Aquí teniu la transcripció dels articles 197 a 201 del Codi Penal (del descobriment i revelació de secrets
    - Artículo 197.
        - 1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.
        - 2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

- **3. Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores. Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior.**

- **4. Los hechos descritos en los apartados 1 y 2 de este artículo serán castigados con una pena de prisión de tres a cinco años cuando:**

  - **a) Se cometan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros; o**

  - **b) se lleven a cabo mediante la utilización no autorizada de datos personales de la víctima.**

- **Si los datos reservados se hubieran difundido, cedido o revelado a terceros, se impondrán las penas en su mitad superior.**

- **5. Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o una persona con discapacidad necesitada de especial protección, se impondrán las penas previstas en su mitad superior.**

- **6. Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado anterior, la pena a imponer será la de prisión de cuatro a siete años.**

- **7. Será castigado con una pena de prisión de tres meses a un año o multa de seis a doce meses el que, sin autorización de la persona afectada, difunda, revele o ceda a terceros**

imágenes o grabaciones audiovisuales de aquélla que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona. La pena se impondrá en su mitad superior cuando los hechos hubieran sido cometidos por el cónyuge o por persona que esté o haya estado unida a él por análoga relación de afectividad, aun sin convivencia, la víctima fuera menor de edad o una persona con discapacidad necesitada de especial protección, o los hechos se hubieran cometido con una finalidad lucrativa.

- **Artículo 197 bis.**
  - **1. El que por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años.**
  - **2. El que mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos, será castigado con una pena de prisión de tres meses a dos años o multa de tres a doce meses.**
- **Artículo 197 ter. Será castigado con una pena de prisión de seis meses a dos años o multa de tres a dieciocho meses el que, sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los apartados 1 y 2 del artículo 197 o el artículo 197 bis:**

- **a) un programa informático, concebido o adaptado principalmente para cometer dichos delitos; o**
- **b) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información.**

- **Artículo 197 quater. Si los hechos descritos en este Capítulo se hubieran cometido en el seno de una organización o grupo criminal, se aplicarán respectivamente las penas superiores en grado.**
- **Artículo 197 quinquies. Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los delitos comprendidos en los artículos 197, 197 bis y 197 ter, se le impondrá la pena de multa de seis meses a dos años. Atendidas las reglas establecidas en el artículo 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 del artículo 33.**
- **Artículo 198. La autoridad o funcionario público que, fuera de los casos permitidos por la Ley, sin mediar causa legal por delito, y prevaliéndose de su cargo, realizare cualquiera de las conductas descritas en el artículo anterior, será castigado con las penas respectivamente previstas en el mismo, en su mitad superior y, además, con la de inhabilitación absoluta por tiempo de seis a doce años**
- **Artículo 199.**
  - **1. El que revelare secretos ajenos, de los que tenga conocimiento por razón de su oficio o sus relaciones laborales, será castigado con la pena de prisión de uno a tres años y multa de seis a doce meses.**
  - **2. El profesional que, con incumplimiento de su obligación de sigilo o reserva, divulgue los secretos de otra persona, será castigado con la pena de prisión de uno a cuatro años, multa de**

doce a veinticuatro meses e inhabilitación especial para dicha profesión por tiempo de dos a seis años.

- Artículo 200. Lo dispuesto en este capítulo será aplicable al que descubriere, revelare o cediere datos reservados de personas jurídicas, sin el consentimiento de sus representantes, salvo lo dispuesto en otros preceptos de este Código.

- Artículo 201.

  - 1. Para proceder por los delitos previstos en este capítulo será necesaria denuncia de la persona agraviada o de su representante legal. Cuando aquélla sea menor de edad, incapaz o una persona desvalida, también podrá denunciar el Ministerio Fiscal.

  - 2. No será precisa la denuncia exigida en el apartado anterior para proceder por los hechos descritos en el artículo 198 de este Código, ni cuando la comisión del delito afecte a los intereses generales o a una pluralidad de personas.

  - 3. El perdón del ofendido o de su representante legal, en su caso, extingue la acción penal sin perjuicio de lo dispuesto en el segundo párrafo del número 5° del apartado 1 del artículo 130.

5.5.- CONTROLAR LES CESSIONS DE DADES

- La relació entre el responsable del fitxer o tractament i l'usuari es bilateral.
- La cessió o comunicació de dades és un tractament de dades que suposa revelar-les a una persona diferent del titular de les dades
- Per tant el responsable del fitxer (cedent) ha de controlar les comunicacions o cessions de dades personals a tercers (cessionaris) per tal que aquestes es facin d'acord amb la llei.
- Cal o bé el consentiment de l'usuari o be que concorri una excepció

- **Un exemple de les cessions habituals d'un fitxer de recursos humans:**

  - **Organismes competents de l'administració de la seguretat social i de l'administració tributària, amb objecte de donar compliment a les obligacions del responsable i dels seus treballadors/usuaris, derivades de la gestió de les nòmines, cotitzacions, expedients laborals i de les obligacions fiscals**

  - **Entitats de protecció social, tals com mútues de protecció laboral i qualsevol entitat a la qual s'encomani el servei de prevenció de riscos laborals o la preservació de la salut dels treballadors/usuaris.**

  - **Entitats financeres en aquells supòsits en els quals els treballadors/usuaris tinguessin establert un sistema de pagament o retribució a través de les esmentades institucions**

  - **Companyies asseguradores o gestores per aquelles assegurances que es tramitin a favor dels treballadors/usuaris tals com assegurances de vida i/o plans de pensió.**

  - **Representants dels treballadors/usuaris, si s'escau, per l'estricte compliment de les seves funcions, tal i com s'estableix en el títol ii del reial decret legislatiu 1/1995 de 24 de març pel que s'aprova el text refós de l'estatut del treballadors.**

  - **Dades de salut o d'afiliació sindical.**

5.6.- TRANSFERÈNCIES INTERNACIONALS DE DADES

- **Molt habitual en el cas de prestació de serveis informàtics (hosting, housing i per tant en tot el fenomen del núvol) per part d'encarregats de tractament.**
- **Una transferència internacional de dades, és un tractament de dades que suposa una transmissió d'aquestes dades fora del territori de l'Espai**

Econòmic Europeu (EEE), tant si constitueix una cessió o comunicació de dades, bé tingui per objecte la realització d'un tractament de dades per compte del responsable del fitxer establert en territori espanyol.

- **L'exportador de dades és la persona física o jurídica, pública o privada, o òrgan administratiu situat en territori espanyol que realitza una transferència de dades de caràcter personal a un país tercer.**
- **L'importador de dades és la persona física o jurídica, pública o privada, o òrgan administratiu receptor de les dades, en cas de transferència internacional d'aquestes dades a un tercer país, tant si és responsable del tractament, encarregat del tractament o tercer.**
- **Les comunicacions de dades en l'EEE constitueixen cessions de dades a efectes de l'aplicació de la LOPD.**
- **Una transferència internacional de dades no exclou en cap cas l'aplicació de les disposicions contingudes en la LOPD i al RLOPD.**
- **Perquè la transferència internacional de dades es pugui considerar conforme al que disposen les esmentades normes, serà necessari autorització del director de l'Agència Espanyola de Protecció de Dades, excepte:**
  - **Que les dades es transfereixin a un país que ofereixi un nivell adequat de protecció**
    - **Suïssa,**
    - **Les entitats nord-americanes adherides als principis de "Port Segur" (safe harbor) declarat nul per sentencia TJCE.**
      - **Ara es diu privacy shield**
        - **https://www.privacyshield.gov/list**
    - **Canadà,**
    - **Argentina,**
    - **Guernsey,**

- **Illa de Man,**
- **Jersey,**
- **Illes Fèroe,**
- **Andorra,**
- **Israel,**
- **Uruguai,**
- **Nova Zelanda**

◦ **o be que concorri algun del supòsits legalment exceptuats de l'autorització del director de l'Agència Espanyola de Protecció de Dades.**

5.7.- ENCARREGAT DEL TRACTAMENT

- **Son persones físiques o jurídiques que presten serveis al responsable del fitxer o tractament:**
  - **L'assessoria fiscal i comptable.**
  - **La gestoria.**
  - **Els advocats.**
  - **Empreses de recobrament de crèdits.**
  - **Call centers (atenció telefònica).**
  - **Empreses d'informàtica (Hosting, Housing, etc)**
  - **Empreses de neteja**
  - **Serveis de videovigilància**
  - **Control d'accés al lloc de treball.**
  - **Serveis de custòdia d'arxius.**
  - **Empreses de destrucció de documentació.**

- **L´APDCAT ha aprovat una recomanació 1/2010**
  - **http://www.apd.cat/ca/contingut.php?cont_id=477&cat_id=128**

- **Cal seguir un conjunt d'obligacions documentades per escrit:**
  - **En tot cas, la realització del tractament per compte de tercers ha d'estar regulada en un contracte que consti per escrit entre el responsable i l'encarregat del tractament.**
  - **L´encarregat de tractament només ha de tractar les dades d'acord amb les instruccions del responsable del tractament.**
  - **No pot utilitzar les dades amb una finalitat diferent de la que figuri en el contracte (no pot enviar publicitat del propi encarregat, per exemple …).**
  - **No pot comunicar les dades a altres persones, ni tan sols per conservar-les (ni subcontractar)**
  - **Està obligat a implementar les mesures de seguretat que es defineixin en el contracte (del mateix nivell que el responsable).**
  - **Està obligat a destruir o tornar al responsable del tractament les dades personals i qualsevol suport o document que contingui alguna dada que hagi estat objecte del tractament, una vegada acomplerta la prestació contractual.**
  - **En el contracte s'han d'establir els mecanismes que el responsable del fitxer utilitzarà per vetllar per tal que l'encarregat del tractament compleixi les seves obligacions**
    - **té els fitxers declarats,**
    - **ha format al seu personal,**
    - **acompleix les mesures de seguretat**
    - **etc.**

6.- LES OBLIGACIONS DEL RESPONSABLE DESPRÉS DEL TRACTAMENT

6.1.- CANCEL·LACIÓ

- Cancel·lació de les dades no vol dir destrucció automàtica, sinó bloqueig de les dades personals durant el termini (depèn en cada cas).
- Després del bloqueig caldrà decidir si s´han de:
  - destruir (automatitzats i no automatitzats). Aplicació de destructores de paper i de dispositius
  - conservar les dades.

7.- ELS DRETS DE L'AFECTAT: A.R.C.O

- L'exercici del drets ARCO és personalíssim, gratuït, són independents entre ells i s'han d'exercir per escrit.

- Dret d'accés:
  - Per conèixer, de manera gratuïta, l'existència dels tractaments de les dades, l'origen i les comunicacions efectuades o que es prevegin fer (article 15 de la Llei orgànica 15/1999, de 13 de desembre, de protecció de dades de caràcter personal, LOPD) en el termini de 30 dies.

- Dret de rectificació:
  - Per corregir les dades personals inexactes o incompletes, en el termini de deu dies (article 16 de la LOPD).

- Dret de cancel·lació (dret a l'oblit):

- **Per donar de baixa les dades personals innecessàries, en el termini de deu dies.**

- **La cancel·lació dóna lloc al bloqueig de les dades, i només s'han de conservar a disposició de les administracions públiques, els jutges i els tribunals, per a l'atenció de possibles responsabilitats nascudes del tractament, durant el termini de prescripció d'aquestes responsabilitats. Complert aquest termini, s'ha de procedir a la supressió (article 16 de la LOPD).**

- **<u>Dret d'oposició al seu tractament:</u>**

  - **Si hi ha un motiu legítim fonamentat relatiu a una situació personal concreta i cap llei no diu el contrari; i també quan es tracti de fitxers amb una finalitat publicitària o de prospecció comercial (article 34 del Reglament de desplegament de la LOPD - Reial decret 1720/2007, de 21 de desembre).**

- **El procediment de tutela de drets.**

8.- LES OBLIGACIONS DEL PERSONAL (document de seguretat)

- **Obligacions que afecten a tot el Personal**

  - **Guardar secret professional i confidencialitat de la informació tractada. Els qui intervinguin en qualsevol fase del tractament de les dades de caràcter personal estan obligats al secret professional respecte de les dades i al deure de guardar-les, obligacions que subsistiran encara després de finalitzar les seves relacions amb el titular del fitxer o, si s'escau, amb el responsable.**

  - **Utilitzar els sistemes d'informació, recursos tècnics així com la informació personal a la qual s'accedeix, únicament per al desenvolupament i exercici professional que l'usuari té assignat.**

  - **Facilitar el dret d'accés, rectificació i cancel·lació als titulars de les dades. Per això s'informarà immediatament al responsable del fitxer, Responsable de Seguretat o encarregat del tractament i es recollirà sempre en sol·licitud escrita.**

- **Funcions i obligacions dels Usuaris**

  - **El personal autoritzat a accedir a la informació de caràcter personal de l'Arxiu, realitzarà les funcions pròpies del seu lloc de treball, que es troben previstes en les relacions de llocs de treball del centre o unitat administrativa a la qual pertanyi, a la corresponent definició de funcions que s'apliqui a aquest personal.**

  - **Contrasenyes**

    - **Cada usuari serà responsable de la confidencialitat de la seva contrasenya i, en cas**

que aquesta sigui coneguda fortuïta o fraudulentament per persones no autoritzades, ha d'enregistrar com a incidència i procedir immediatament al seu canvi.

- Cada usuari haurà de canviar la contrasenya inicial que se li assigni, en el primer accés que realitzi al sistema o després del desbloqueig de la seva contrasenya quan hagi estat necessària la intervenció d'una tercera persona en aquest procés.

- Les contrasenyes han de ser prou complexes i difícilment endevinables per tercers, evitant l'ús del propi identificador com contrasenya o paraules senzilles, el nom propi, data de naixement etc.

- Per això s'han de seguir les pautes en l'elecció de les contrasenyes:

  - hauran de tenir una longitud mínima de 8 caràcters alfanumèrics.
  - no hauran de coincidir amb el codi d'usuari.
  - no han d'estar basades en cadenes de caràcters que siguin fàcilment associades a l'usuari (nom, cognoms, ciutat i data de naixement, noms de familiars, matrícula del cotxe, etc.)

- L'usuari haurà d'aplicar regles mnemotècniques per poder construir una contrasenya prou difícil d'endevinar per tercers i que alhora sigui molt fàcil de recordar per ell.

◦ Llocs de treball

- Els llocs de treball estaran sota la responsabilitat d'algun usuari autoritzat que garantirà que la informació que mostren no pugui ser visible per persones no autoritzades.

- Tant les pantalles com les impressores o altres tipus de dispositius connectats al lloc de treball hauran d'estar físicament ubicats en llocs que garanteixin aquesta confidencialitat.

- **Quan el responsable d'un lloc de treball l'abandoni, bé temporalment o bé en finalitzar el seu torn de treball, haurà de deixar en un estat que impedeixi la visualització de les dades protegides, com per exemple un protector de pantalla amb contrasenya. La represa del treball implicarà la desactivació de la pantalla protectora amb la introducció de la contrasenya corresponent.**

- **En el cas de les impressores s'ha d'assegurar que no queden documents impresos a la safata de sortida que continguin dades protegides. Si les impressores són compartides amb altres usuaris no autoritzats per accedir a les dades del fitxer, els responsables de cada lloc hauran de retirar els documents a mesura vagin impresos.**

- **Queda expressament prohibit qualsevol canvi de la configuració de la connexió dels llocs de treball a xarxes o sistemes exteriors, que no estigui autoritzat expressament pel responsable del fitxer o el director del centre o departament al qual pertanyi cada usuari. La revocació d'aquesta prohibició ha de ser autoritzada expressament.**

- **Els llocs de treball des dels quals es té accés al fitxer tindran una configuració fixa en les seves aplicacions, sistemes operatius que només pot canviar sota l'autorització del responsable de seguretat o per administradors autoritzats de l'annex F.**

◦ **Fitxers Temporals**

- **Queda expressament prohibit el tractament dades extretes de l'Arxiu, amb programes ofimàtics, com processadors de text o fulls de càlcul, sense comunicar per esser aprovat al responsable del Seguretat perquè es procedeixi a implantar les mesures de seguretat adequades.**

- **La utilització d'aquests programes per al tractament de dades personals sense comunicar-ho al responsable de Seguretat serà considerat com una falta contra la seguretat del fitxer per part d'aquest usuari.**

- **S'haurà evitar el guardar còpies de les dades personals del fitxer en arxius intermedis o temporals.**

- **En el cas que sigui imprescindible realitzar aquestes còpies temporals per exigències del tractament, caldrà adoptar les següents precaucions:**

  - **Realitzar sempre aquestes còpies sobre un mateix directori de nom TEMP o similar, de manera que no quedin disperses per tot el disc de l'ordinador i sempre es pugui conèixer on estan les dades temporals.**

  - **Després de realitzar el tractament per als quals han estat necessaris aquestes dades temporals, procedir a l'esborrat o destrucció dels mateixos**

  - **Els fitxers temporals creats exclusivament per a la realització de treballs temporals o auxiliars han de complir el nivell de seguretat que els correspongui d'acord amb els criteris expressats en el Reglament de Mesures de Seguretat.**

◦ **Treball fora dels locals**

- **No s'ha de copiar ni transportar informació dels sistemes centrals en portàtils o estacions de treball que es trobin fora de les oficines sense la corresponent autorització del responsable del fitxer. A l'Annex G es referència un procediment per al tractament de fitxers fora de la seva ubicació, com és el cas dels ordinadors portàtils.**

◦ **<u>Incidències</u>**

- **Qualsevol usuari que tingui coneixement d'una incidència és responsable de la comunicació de la mateixa al responsable de Seguretat o al responsable del fitxer o la persona encarregada de registrar-la. En el cas que el procediment d'Incidències estigués automatitzat, haurà de**

procedir al seu registre en el sistema habilitat. El model de notificació d'incidències figura en l'annex I.

- **El coneixement i la no notificació d'una incidència per part d'un usuari serà considerat com una falta contra la seguretat del Fitxer per part d'aquest usuari.**

◦ **<u>Gestió de suports i annexos</u>**

- **Quan un usuari gestioni o produeixi suports que continguin dades de l'Arxiu, bé com a conseqüència d'operacions intermèdies pròpies de l'aplicació que els tracta, o bé com a conseqüència de processos periòdics de suport o qualsevol altra operació esporàdica, aquests han d'estar clarament identificats amb una etiqueta externa que indiqui de quin fitxer es tracta, quin tipus de dades conté, procés que els ha originat i data de creació.**

- **Quan es reciclin mitjans que siguin reutilitzables, i que hagin contingut còpies de dades de l'Arxiu, hauran de ser esborrats físicament abans de la seva reutilització, de manera que les dades que contenien no siguin recuperables. Aquells que no hagin de ser reutilitzats s'han de destruir mitjançant un procediment especificat en l'annex G.**

- **Els suports que continguin dades de l'Arxiu hauran de ser emmagatzemats en llocs al que no tinguin accés persones no autoritzades per a l'ús del Fitxer.**

- **La sortida de suports informàtics que continguin dades de l'Arxiu fora dels locals on està ubicat el Fitxer ha de ser expressament autoritzada pel responsable del Fitxer mitjançant el procediment descrit en l'Annex G.**

- **Només es podran realitzar enviaments del fitxer, per correu electrònic o transferències electròniques, des d'un únic compte o adreça de correu controlat per un usuari especialment**

autoritzat pel responsable o persona autoritzada com es descriu en l'annex G.

- **Hi haurà un compte o adreça de correu electrònica controlada per un usuari especialment autoritzat, per rebre dades del fitxer.**

- **Es deixarà constància de totes les sortides i entrades de dades del fitxer a través de correu electrònic, en directoris històrics d'aquesta adreça de correu o en algun altre sistema de registre de sortides i/o entrades que permeti conèixer en qualsevol moment els enviaments realitzats o rebuts, a qui anaven dirigits, o els remitents i la informació enviada, tal com s'indica en procediment que s'ha d'adjuntar a l'Annex G.**

- **Quan les dades del Fitxer hagin de ser enviats fora del recinte físicament protegit on es troba ubicat el fitxer, bé sigui mitjançant un suport físic d'enregistrament de dades o bé a través de correu electrònic, han de ser xifrats o bé s'utilitzarà qualsevol altre mecanisme que asseguri que aquesta informació no sigui accessible o manipulada durant el seu transport. A l'Annex G s'especificarà el procediment.**

- **S'han de xifrar les dades que continguin els ordinadors portàtils quan aquests es trobin fora de les instal·lacions que estan sota el control del responsable, si això no és possible es farà constar el procediment que ha de figurar en l'annex G. A l'Annex G, s'especificarà el procediment.**

◦ **<u>Transmissió de dades a través de xarxes</u>**

- **La transmissió de dades de caràcter personal de nivell alt a través de xarxes de públiques telecomunicacions o sense fils o la sortida o distribució de suports amb dades de nivell alt fora, es realitzarà xifrant les dades o bé utilitzant qualsevol altre mecanisme que garanteixi que la informació no sigui intel·ligible ni manipulada per tercers. A l'Annex G, s'especificarà el procediment.**

9.- LA RESPONSABILITAT

9.1.- ASPECTES CIVILS

- Regulat a l´article 19 de la LOPD
- Suposa demanar una indemnització al responsable del fitxer o tractament (sobretot és habitual en els fitxers de solvència patrimonial i crèdit).

9.2.- ASPECTES PENALS

- STS 18 de febrer de 1999.
  - Periodista que había publicado la noticia de que en la cocina de una prisión (el salto del negro) trabajaban dos presos con sida, cuyos nombres completos revelaba: Sida, cocina y cárcel
  - En la prisión Provincial del Salto del Negro corre el rumor insistente de que hay al menos dos presos con sida que están destinados en el servicio de cocina, con lo que la alarma entre los internos y los funcionarios está creciendo.
  - Este periódico ha tenido acceso a un listado de reclusos con destino específico en la cocina del centro penitenciario y otro con el nombre de los internos que padecen sida.
  - En ambas listas se repiten dos nombres, J.M.G.S. [nombre y apellidos completos de uno de ellos], nacido en [lugar de nacimiento], el [fecha completa], soltero y [...] de profesión, con varios ingresos y dado de alta en la cocina el [fecha completa], y J.O.G.M. [nombre y apellidos completos del otro preso], nacido en [lugar de nacimiento], soltero y condenado por [delito contra la libertad sexual], dado de alta en la cocina el [fecha].”
  - El Tribunal Supremo revocó la Sentencia de la Audiencia Provincial de Las Palmas y dictó nueva Sentencia en la que condenó al acusado, como autor responsable de un delito del art. 197.2, 3

y 5, con la eximente incompleta de ejercicio legítimo de un derecho, a la pena de un año de prisión, multa de doce meses e inhabilitación especial para el ejercicio de la profesión de periodista durante un año; así como al pago de dos millones de pesetas a J.M.G.S. y a J.O.G.M. que, en caso de insolvencia, deberían ser abonados por la empresa Editorial Prensa Canaria S.A.

9.3.- ASPECTES ADMINISTRATIUS

- **Els fitxers publics no tenen sanció económica.**
- **Els fitxers privats si:**
  - **Sancions econòmiques fins a 600.000 euros**

9.4.- ASPECTES LABORALS

- **Sentència del T.S.J Andalucia/Granada de 22-05-2001**
  - **Declara procedent l'acomiadament d'un treballador d'un banc, que va accedir a dades bancàries d'un client amb el que no tenia relació professional alguna per raó del càrrec que ocupa i per tant, sense altra raó que la de conèixer a títol personal els moviments del compte.**

10.- EL PROTOCOL D'ÚS DE LES TECNOLOGIES DE LA INFORMACIÓ

- **Establir les normes d'ús de les tecnologies a l'empresa o Administració Pública per tal d'adequar l'ús dels recursos per part dels usuaris a la sentència del Tribunal Suprem, sala 4ª de lo social, de 26-09-2007 i altra normativa concurrent.**
  - **Es regula:**
    - **la clau d'usuari (nom i contrasenya).**
    - **els recursos.**
    - **la navegació per Internet.**
    - **el correu electrònic (corporatiu i particular).**
    - **llistes de distribució.**
    - **els espais físics.**
    - **el programari.**
    - **facultat de control.**
    - **incidències, dubtes i suggeriments.**
    - **pèrdua de la condició d'usuari.**
    - **coneixement del document.**

11.- DECÀLEG PER LA PROTECCIÓ DE DADES PERSONALS

- Aquí teniu una llista creada per l'Autoritat Basca de Protecció de Dades que és com un recordatori:
  - http://www.avpd.euskadi.net/

- RECORDA QUE LES DADES SÓN DE LES PERSONES
  - Les dades personals (informació numèrica, alfabètica, gràfica, fotogràfica o acústica sobre persones) pertanyen a les persones a les quals es refereixen i només elles poden decidir sobre aquests.
  - Per tant, ni tu, ni el teu servei, ni el teu departament sou amos d'elles.

- PER COMENÇAR, COMPROVA QUE EL FITXER ESTÀ CREAT
  - Cal que comprovis que el fitxer està creat, és a dir, que està inscrit al Registre de Protecció de Dades i que hi ha una persona responsable del fitxer i una responsable de seguretat, que han de resoldre els dubtes que se't presentin.

- INFORMA I DEMANA EL CONSENTIMENT
  - Quan sol·licitis dades personals, has informar-los de l'existència del fitxer, la seva finalitat, etc.
  - Per a això has d'utilitzar els formularis que s'han preparat.
  - En alguns casos serà necessari, a més, que sol·licitis el consentiment exprés del ciutadà per tractar les seves dades.

- SOL·LICITA I TRACTA NOMÉS DADES ADEQUADES, PERTINENTS I NO EXCESSIVES

- Les dades personals han de ser adequades, pertinents i no excessives amb relació a la finalitat per a la qual es recullen.
- No pots utilitzar dades personals recollides per a finalitats incompatibles amb aquelles per a les quals es van recollir.

- **COMPLEIX LES MESURES DE SEGURETAT**
  - És la teva obligació complir la normativa de seguretat en matèria de dades personals.
  - Si no te l'han lliurat, has reclamar al responsable de Seguretat.
  - No t'oblidis de:
    - Utilitzar les contrasenyes i no compartir-les.
    - Guardar els expedients o llistats amb dades personals en armaris, que tancaràs quan no estiguis.
    - Mantenir les dades personals fora de la vista de persones no autoritzades (atenció als documents que deixes en fotocopiadores, impressores, faxos o, fins i tot, damunt de la taula).
    - Complir les mesures de seguretat si et portes dades en memòries USB o altres suports.

- **FACILITA L'EXERCICI DE DRETS "ARCO" A LES PERSONES A LES QUE ES REFEREIXEN LES DADES**
  - Has de facilitar a la persona titular de les dades personals el dret a Accedir, Rectificar, Cancel·lar i Oposar-se al tractament de les seves dades.
  - Hauràs de saber informar sobre com exercir-los i facilitar-impresos perquè pugui fer-ho.

- **COMPLEIX AMB EL TEU DEURE DE SECRET**

- Mantingues, indefinidament, absoluta reserva i sigil sobre qualsevol informació personal a la qual accedeixis en l'exercici de les teves funcions.

- Et obliguen a això la normativa de protecció de dades i una ètica de conducta bàsica. De vegades, el seu incompliment, pot ser perseguit penalment.

- **NO CEDEIXIS DADES SENSE AUTORITZACIÓ**

  - No cedeixis mai dades personals a altres Administracions, entitats o particulars sense autorització de la persona responsable del fitxer o del responsable de Seguretat.

- **COMPROVA QUE EXISTEIXI UN CONTRACTE AMB EMPRESES QUE TREBALLEN PER LA TEVA ADMINISTRACIÓ O EMPRESA**

  - Abans de facilitar dades personals a empreses o entitats que, en virtut de contractes, realitzen treballs per la teva organització (desenvolupaments informàtics, seguretat, neteja, distribució de correspondència, ...) assegura't que hi ha un contracte signat on se'ls imposen obligacions de confidencialitat i de seguretat de la informació respecte a les dades de caràcter personal.

- **QUAN NO SIGUIN NECESSÀRIES, CANCEL·LA LES DADES DE MANERA ADEQUADA**

  - Cancel·la les dades quan deixin de ser necessàries o pertinents per a la finalitat per la qual van ser recollides.

  - Algunes vegades, abans de destruir caldrà bloquejar, és a dir, impossibilitar el tractament i permetre l'accés només quan es donin algunes situacions concretes.

  - Per destruir fitxers amb dades personals en suport paper utilitza les destructores de paper o el sistema segur que hi ha establert la teva organització

Moltes gràcies !